

REMARKS

Claims 1-29 are pending in this application. Claims 1, 5, and 18 are amended herein. Support for the amendments to claims 1, 5, and 18 may be found in claims 1, 5, and 18 as originally filed. Since the amendments to the claims merely provide antecedent bases for existing elements, they are not made for any reason of patentability. New claim 29 is added herein. Support for new claim 29 may be found in claim 1 as originally filed. Reconsideration is requested based on the foregoing amendment and the following remarks.

Response to Arguments:

The Applicants appreciate the consideration given to their arguments. Further consideration is thus requested.

Claim Rejections - 35 U.S.C. § 112:

Claims 1-28 were rejected under 35 U.S.C. § 112, second paragraph, as indefinite. Claims 1, 5, and 18 were amended to make them more definite. Withdrawal of the rejection is earnestly solicited.

Claim Rejections - 35 U.S.C. § 103:

Claims 1-7, 9, 11, 13, 18, 19, 21, 23, and 25-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,392,351 to Hasebe et al., (hereinafter "Hasebe"), in view of U.S. Patent No. 5,892,900 to Ginter et al. (hereinafter "Ginter"), UK Patent Application GB 2 284 689 to Chen (hereinafter "Chen"), and U.S. Patent Application No. 2001/0042043 to Shear et al. (hereinafter "Shear"). The rejection is traversed. Reconsideration is earnestly solicited.

Claim 1 recites,

"storing the encrypted predetermined information in an area outside said predetermined secure area."

Neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1. Thus even if Hasebe, Ginter, Chen, and Shear were combined, as proposed in the Office Action, the claimed invention would not result.

The Office Action, in fact, acknowledges Hasebe shows no storage of encrypted

predetermined information in an area outside a predetermined secure area. The Office Action seeks to compensate for this deficiency of Hasebe by combining Hasebe with Chen, saying that backing up an IC card as described in Chen at page 1, paragraphs [0001]-[0003] is equivalent to storage of encrypted predetermined information in an area outside a predetermined secure area. This is submitted to be incorrect.

Backing up an IC card, rather, is not the same as “storing the encrypted predetermined information in an area outside said predetermined secure area,” as recited in claim 1. In the first place, the IC card of Chen really has no encrypted predetermined information to store. Rather, as described page 1, lines 6, 7, and 8 of Chen,

Most portable data providing devices, such as electronic dictionaries, employ an IC card to expand its database or to upgrade the functions of the same.

The IC card of Chen is thus employed to expand databases or to upgrade the functions of portable data providing devices, such as electronic dictionaries, not “storing the encrypted predetermined information in an area outside said predetermined secure area,” as recited in claim 1. No mention of encryption appears in Chen at all.

Ginter, for its part, shows no “storing the encrypted predetermined information in an area outside said predetermined secure area,” as recited in claim 1, either. In Ginter, rather, as described at column 173, lines 30-33,

Instead, back up routine 1250 encrypts each secure database 610 item with a newly generated back up key(s) (block 1256) and writes the encrypted item to back up store 668 (block 1258). This process continues until all items within secure database 610 have been read, decrypted, encrypted with a newly generated back up key(s), and written to the back up store (as tested for by decision block 1260).

Thus, Ginter doesn't even bother trying to figure out what the encryption key held by SPU 500 might have been, let alone “storing the encrypted predetermined information in an area outside said predetermined secure area,” as recited in claim 1. Ginter, rather, just creates new encryption keys whenever it needs them.

Finally, Shear shows no “storing the encrypted predetermined information in an area outside said predetermined secure area,” as recited in claim 1, either. In Shear, rather, as described at paragraph [0218],

In the example shown in FIG. 3, disk 100 stores one or more decryption keys for decrypting key block 208 on the medium itself in the form of a hidden key(s) 210. Hidden key(s) 210 may be stored, for example, in a location on disk 100 not normally accessible.

Thus, hidden key(s) 210 of Shear are stored in an inaccessible, i.e. secure location on disk 100, rather than “storing the encrypted predetermined information in an area outside said predetermined secure area,” as recited in claim 1. Or, in the alternative, as described in Shear at paragraph [0219],

Alternatively, and/or in addition, keys required to decrypt encrypted key block 208 could be provided by disk drive 80. In this example, disk drive 80 might include a small decryption component such as, for example, an integrated circuit decryption engine including a small secure internal key store memory 212 having keys stored therein. Disk drive 80 could use this key store 212 in order to decrypt encrypted key block 208 without exposing either keys 212 or decrypted key block 208--and then use the decrypted key from key block 208 to decrypt protected content 200, 202.

This is to be contrasted with claim 1, which recites “storing the encrypted predetermined information in an area outside said predetermined secure area.” Thus, even if Hasebe, Ginter, Chen, and Shear were combined, as suggested by the Office Action, the claimed invention would not result.

Furthermore, persons of ordinary skill in the art who read Hasebe for all it contained at the time the invention was made would have been deterred from modifying Hasebe in the manner proposed in the Office Action and thus, even if the combination included the elements of the claimed invention, it would not have been obvious. Hasebe, in particular, warns against illegal copying at column 1, lines 18-24, where he notes,

However, it is relatively easy for a third party to illegally copy electronic data. As a result of illegal copying, a vendor of electronic data suffers significant damage in that he cannot derive legitimate benefits. As a result of this damage, the cost of electronic data, i.e., the software and electronically published data rises so that users also suffer due to increased prices.

Copying software illegally is technically equivalent to copying software for back-up purposes. Copying is copying. The computer will never know the difference. The only difference between making an illegal copy of software and backing up software is the intention of the copier. Furthermore, the economic effect of which Hasebe warns are the same in each case, the vendor of electronic data derives no benefits, legitimate or otherwise, from the backed-up software, either. The vendor would certainly prefer that a customer bought back-up copies from the vendor, rather than making them themselves. Therefore, persons of ordinary skill in the art would have not been motivated to combine the references as suggested by the Office Action, since Hasebe warns against (illegal) copying. Claim 1 is submitted to be allowable. Withdrawal of the rejection of claim 1 is earnestly solicited.

Claims 2-7, 9, 11, 13, and 27 depend from claim 1 and add additional distinguishing elements. Claims 2-7, 9, 11, 13, and 27 are thus also submitted to be allowable. Withdrawal of the rejection of claims 2-7, 9, 11, 13, and 27 is earnestly solicited.

Claims 18, 19, 21, 23, 25, 26, and 28:

Claim 18 recites,

“storing the encrypted predetermined information in an area outside said secure area.”

Neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest “storing the encrypted predetermined information in an area outside said secure area,” as discussed above with respect to claim 1. Claim 18 is thus submitted to be allowable as well, for at least those reasons discussed above with respect to claim 1. Withdrawal of the rejection of claim 18 is earnestly solicited.

Claims 19, 21, 23, 25, 26, and 28 depend from claim 18 and add additional distinguishing elements. Claims 19, 21, 23, 25, 26, and 28 are thus also submitted to be allowable. Withdrawal of the rejection of claims 19, 21, 23, 25, 26, and 28 is earnestly solicited.

Claims 8, 10, 12, 14-17, 20, 22, and 24:

Claims 8, 10, 12, 14-17, 20, 22, and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hasebe, Ginter, Chen, and Shear, and further in view of U.S. Patent No. 5,191,611 to Lang. (hereinafter “Lang”). The rejection is traversed. Reconsideration is earnestly solicited.

Claims 8, 10, 12, and 14-17 depend from claim 1 and add additional distinguishing elements. Neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest “storing the encrypted predetermined information in an area outside said secure area,” as discussed above with respect to claim 1. Lang shows no “storing the encrypted predetermined information in an area outside said predetermined secure area,” either, and thus cannot compensate for the deficiencies of Hasebe, Ginter, Chen, and Shear with respect to claims 8, 10, 12, and 14-17. In Lang, rather, as described at column 2, lines 42-47,

Additionally, a storage accessing device (used interchangeably herein with the following terms--personal accessing device (PAD) and smart card) provided with an encrypted or non-encrypted personal security key as well as personal identification code is included to allow an individual access to the storage medium or media.

Thus, a storage accessing device in Lang is provided with an encrypted or non-encrypted

personal security key. No mention “storing the encrypted predetermined information in an area outside said predetermined secure area,” as recited in claim 1, appears in Lang at all.

Or else, as described at column 4, lines 2-8,

Alternatively, the decryption algorithm can be stored on the smart card and the decryption of information would take place in the smart card and this information is then transferred to the computer for viewing and processing.

This is to be contrasted with claim 1, which recites, “storing the encrypted predetermined information in an area outside said predetermined secure area.” Claims 8, 10, 12, and 14-17 are thus also submitted to be allowable. Withdrawal of the rejection of claims 8, 10, 12, and 14-17 is earnestly solicited.

Claims 20, 22, and 24:

Claims 20, 22, and 24 depend from claim 18 and add additional distinguishing elements. Neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest “storing the encrypted predetermined information in an area outside said secure area,” as discussed above with respect to claim 1. Lang shows no storage of encrypted predetermined information in an area outside a predetermined secure area either, and thus cannot compensate for the deficiencies of Hasebe, Ginter, Chen, and Shear with respect to claims 20, 22, and 24. Claims 20, 22, and 24 are thus also submitted to be allowable. Withdrawal of the rejection of claims 20, 22, and 24 is earnestly solicited.

New claim 29:

New claim 29 recites,

“storing information encrypted with medium-specific information or a key generated therefrom in an area outside a secure area.”

None of the references cited recite “storing information encrypted with medium-specific information or a key generated therefrom in an area outside a secure area,” as recited in new claim 29. New claim 29 is thus believed to be allowable.

Conclusion:

Accordingly, in view of the reasons given above, it is submitted that all of claims 1-29 are allowable over the cited references. Allowance of all claims 1-29 and of this entire application is therefore respectfully requested.

Serial No. 09/800,505

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 29 NOV 05

By:


Thomas E. McKiernan
Registration No. 37,889

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501